25 Nov 1968

The attached descriptions represent an incomplete effort of consolidating various agency responses re outlining computer security problem areas in each agency.

COMPUTER SECURITY PROBLEM AREAS

I. USER IDENTIFICATION

DIA — User Authentication/Identification

Comment: An authentication system is currently being developed which is intended to insure against inadvertent release of classified information to unauthorized persons. Each DIA user of the system is to be identified to the system by a specifically assigned "user's authentication number." This number will be the passage whereby a user is allowed "need-to-know" retrieval access to an information data base, and whereby he is allowed or denied the privilege to access and modify a data base. Responsibilities and procedures for assigning and administering this number is yet to be established.

ACSI — Army does not comment directly on "users". Army's listed heading: "Files Integrity, Multi-user" may apply here, however, is not further defined.

Air Force — AF does not comment directly on "users." AF comments under "Integrity of Files" may apply here, but are listed under next topic.

Navy — Although Navy does not comment directly, its Receipting topic may apply here.

Comment: Receipting - to include a method (i.e. a log of transactions) indicating that classified information provided any user by the system

Note: Other comments by Navy under (1) Protection at Boundaries, and (2) Identification of Classification may apply under the topic User Identification.

25X1

NSA — Identification of User

Comment: Assurance must be made that only those users authorized to have access will receive the desired information. In addition to clearance determination, such things as code name compartmented name, handling caveats, etc., must be given consideration to insure proper need-to-know.

AEC — Authorized User Identity Code

AEC regulations discuss a train of alpha-numerical characters assigned to a user of the system authorizing access to classified files. It also discusses File Identity Code for a file of data and a Master Recognition File made up of the authorized users identity code, the file identity code, and the station access. (See Security Controls for classified remote access computer systems pp. 8 through 16.)

II. FILE INTEGRITY

DIA : DIA does not comment on this topic directly but its comments on user identification may apply here.

NSA : Protection of the Information or Files of the Computer System Comment: Since files may contain information of different levels of sensitivity and/or classification, the access to these files by users must be rigidly controlled.

Army : (b) File Integrity, multi-user.
(c) Program Integrity.
(NOTE: These topics are not defined.)

AF : 2. The Integrity of Individual Files and Executive Programs Comment: It is believed that the protection of individual files and executive programs must be made a part of the software through use of key words, lock outs, etc. At present it has been accomplished to a limited degree by writing in legal and illegal queries or actions. This technique can be inordinately complicated, time consuming and wasteful of storage space.

Navy : Navy does not comment directly on this topic but its comments on "Protection of Boundaries" may be applicable here.

III. SANITIZATION OF STORAGE MEDIA

ACSI : Sanitization of Storage Media:

(1) Disc.
(2) Drum.
(3) Core.
(4) Magnetic Tape.
(5) Magnetic Cards.

AF : The Requirement to Sanitize Computer Tapes, Disks, Disk Packs & Drums

Comment: Degaussing works well for tapes containing non-compartmented information. Because of relatively low cost, physical destruction of tapes containing compartmented information is feasible. However, this situation does not apply to sanitization of disks, disk packs and drums when compartmented information is involved. In these cases destruction of the disks, disk pack or drum seems to be the only, and very costly, answer since degaussing and overprinting is apparently not recognized as being adequate.

Navy : (1) Downgrading & declassification of disc, drums and tapes.

(2) Stowage of tapes, drums & discs.

Comment: There is an introductory comment under heading of Collateral Problems.

State : File Keeping

Comment: As volume increases in tapes, reels, and discs, causing storage problems, do we enlarge storage area or discard, degause & reuse?

CIA : Degaussing on Storage Media

Comment (Synopsis of pp 18 & 19 in IBSEC-M-104):

One of current adjunctive problems is that of degaussing storage media. Degaussing to be secure means reducing retrievability of the magnetically coded data to a degree that it is prohibitively difficult. Degaussing problem in ADP environment are presented not only by the magnetic tapes but also disc and drum storage devices, and even main memory itself. Adequate means have been devised to permit degaussing of magnetic tapes to a degree that they may be considered unclassified after established procedures have been executed with approved degaussing .... Acceptable procedures must be developed to permit degaussing of disc and other storage devices. The problem also relates to "working space" utilized in the computer operation itself. Here, however, it appears that adequate overwrite procedures may suffice to solve the problem, praticularly since it is as much a technical problem as a security one ....

IV. CLASSIFICATION OF INFORMATION

DIA: Over Classification of Information

Comment: Under the present mode of operation, clearance is required of all personnel involved in the system. This includes operators, maintenance personnel, technicians, and users. All information processed through the system is considered SI. This poses a problem in that it restricts the use of information to the few who have the appropriate clearance and denies proper maintenance and efficient functioning of the system.

ACSI: Co-Location of Intelligence Data Handling Systems handling SI Material with Command and Control systems not indoctrinated for SI.

Comment: No other details given.

Air Force: The possibility of Co-Locating Command & Control and Intelligence Data Handling System.

Comment: JCS are considering policy guidance on co-location. Should this materialize and co-location as addressed becomes a reality, it would not necessarily mean joint use of a single computer. However future installations would almost surely be required to use the same equipment. Such situations would impinge on all aspects of computer security and personnel security forcing the entire facility to be upgraded from the overall security point of view.

Navy: Identification of Classification

Comment: An adequate means (is needed) of notifying users of the classification level of the information furnished to them by the system.

Receipting: To include a method (i.e., a log of transactions) indicating classification of information provided any user by the system. (NOTE: This topic was previously listed under User Authentication/Identification)

NSA: Classification of Information Derived from Multi-Sources

Comment: Topic is not further defined.

AEC: Security Controls for Classified Remote Access Computer Systems.

Comment: Page 4 of AEC regulation discusses the purpose of controls and limitations regarding TOP SECRET information transmission from remote terminals to CPU.

CIA: Security Classification & Dissemination Controls

Comment: The need to include identification by security classification and the dissemination controls are noted for information stored, processed and created by ADP methods.

State: Transportation of classified punch cards is discussed as to problems encountered in following usual shipping and wrapping required by regulations for traditional classified information shipments.

V. ACCESS TO COMPUTER OPERATIONS

DIA: This topic is discussed under Physical Security.

Comment: The problem of physical security will be made greater because of the eventual wealth of information stored in one place. Needless to say, a more determined effort will possibly be made by hostile intelligence services. It will be necessary that intrusion devices and other approved methods of controlling access be the best available. Testing of the various methods of security will require additional manpower due to the necessity for closer intervals in discussing these tests.

ACSI: This topic may be inferred in the topic Personnel Security (larger numbers, less supervision). The topic is not further defined.

Air Force: (a) The requirement for Physical Security of the ADP equipment, installation and Personal Security clearances and access authorizations for the facilities personnel.

Comment: Here we are faced with several real or imagined problems. The elementary steps are obviously taken care of by restricted areas, locks, guards and other authorized access controls.

(b) Air Force comments on co-location problem, notes that "joint use" will result in forcing (personnel security) be upgraded."

Navy: (a) Remote Devices

Comment: The physical security and access control required at remote input and output device installations.

(b) Navy also discusses under its heading of Collateral Problems, the topic: Personnel Access Control. This is not further defined.

NSA: (a) Clearance of Operating Personnel
--Required level & need-to-know
Comment: The problem of controlling need-to-know in multi-level/multi-access computer systems becomes more complex.

(b) Providing adequate physical security safeguards in storage and computer areas. (This is not further defined.)

AEC: AEC regulations provide for Physical Security and Personnel Security under these topics. They also provide under Security Controls for classified remote access computer systems for:

(a) Computer Security Control Officer (page 18)

(b) Physical Security Measures for Central Processing Area (page 19)

(c) Physical Security Measures for Remote Access Stations Processing Classified Information (page 22)

CIA: (Physical Security and Personnel Security problems are not included in the problems in ADP on the distinction that these types of problems are adequately handled under traditional security procedures.) Under ADP: The topic Storage Problems. There is a discussion of the Mass Storage Probelm with Vulnerability of Volume of Data in Small Area.

Under the topic Adjunctive Problems there is a discussion of "Remote Terminal Vulnerability".

(These topics are discussed in detail on pages 12 & 13 in "A Presentation on Security in the Automatic Data Processing Environment.")

VI. COMMUNICATIONS SECURITY

DIA: Communications Security

Comment: Adequate safeguards must be established to insure that the system is provided an operational environment which presents no hindrance to efficient and effective performance. Telephones, radios or any "foreign" transmitting devices must be given more than normal concern. Consideration should be given to prohibiting such instruments in areas where ADP equipment is located. Every effort must be made to prevent machine error, human error and cross talk. Equipment such as Model 33 TTY, should not be located in the same area as the ADP equipment.

ACSI: Security of Communications; TEMPEST

(These problem areas are not further defined in this paper but the "TEMPEST control measures for ADP Systems & Equipment" gives full details.)

Air Force: (a) The requirement for communications security

Comment: This problem involves both the security of communications between computers, and between computers and remote query devices. Encryption devices, line shielding & the use of special key words, codes, lock outs, etc., may provide the solution.

(b) Under the caption on physical security Air Force also notes: "It is recognized that computer emissions are a reality. However, are these emissions really a security problem? How serious is this problem? (By Hearsay, the IBM 360 generation computer can be intercepted for a considerable distance. However, it has been said that it would take an identical IBM 360 computer 10 years to translate the intercepted data into intelligible information.) This area should be explored and clarified. We need answers to the questions: Are Computer emissions a security problem? How much of a problem? Will shielding work? Is the risk worth the cost of shielding? "

Navy: TEMPEST (See "TEMPEST Control Measures for ADP Systems & Equipment.)

NSA: (a) Protection ot communication links & equipment from emanation and possibly direct line taps.

(b) Insuring that proper safeguards are maintained to prevent override or cross talk within the hardware of the system.

AEC: (a) AEC regulations include complete description ot installation & maintenance requirements for protected wirelines.

(b) AEC computer security outline ot basic problems lists:

(1) Emission Security
(2) Crypto Security
(3) Transmission Security.

CIA: Under the topic Operational Type Problems the following are listed:

(1) Electro-Magnetic Radiation
(2) Wiretapping

(Details of radiation & wiretapping points of greatest vulnerability are discussed on Page 14 in "A Presentation on Security in the ADP Environment.")

VII. SPILLAGE--INADVERTENT DUMP

DIA: No direct topic but in discussing Communications Security the comment is noted "Every effort must be made to (control) machine error, and cross talk. Equipment, such as Model 33 TTY should not be located in the same area as the ADP equipment."

ACSI: Unauthorized Disclosure (Spillage)
Not further defined.

Air Force: The requirement to prevent the Inadvertent "Dump" of information.

Comment: In the past, this has not been a particular problem, but with the introduction of third generation computers and remote query devices capable of simultaneous operation this is now a problem. Here the problems of "need to know" and inadvertent disclosure become the greatest. Inadvertent "dump" through design or accident is both possible and probable regardless of the safeguards created in the software of the system. We don't even pretend to have the answer for this problem.

Navy: Multi-level remote terminal installations. One of the specific problems: Inadvertent Dump. The (need is also cited for) protection necessary against intentional tampering, spurious altering or loss of data.

NSA: Insuring that proper safeguards are maintained to prevent override or cross talk within the hardware of the system.

AEC: There is no direct comment on this topic but under AEC Regulations "Security Controls for Classified Remote Access Computer Systems" a topic is discussed under System Capability that the system disallows additional inquiries from a remote station it two improper inquiries are attempted within 30 minute period. (Although this appears to be aimed at penetration, this could be inadvertent inquiry & response.)

CIA: Under the topic "Operational Type Problems" -- Spillage and penetration in a multi-level system are discussed under the heading: Accidental Spillage and Deliberate Penetration.
(NOTE: Detailed discussion of these topics are on pages 16 and 17 of "A Presentation on Security in the Automatic Data Processing Environment.")